

БЕЗОПАСНОСТЬ СЛОЖНЫХ ЭКОНОМИЧЕСКИХ СИСТЕМ: УПРАВЛЕНИЕ РИСКАМИ ИХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ*

Владимир Яковлевич ЗАХАРОВ ^a,

Елена Николаевна ЛУДУШКИНА ^{b,*},

Елена Валерьевна КОРНИЛОВА ^c,

Марина Владимировна КИСЛИНСКАЯ ^d

^a доктор экономических наук, профессор кафедры экономики предприятий и организаций, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского (ННГУ), Нижний Новгород, Российская Федерация
zakharov48@yandex.ru
<https://orcid.org/0000-0001-6402-4827>
SPIN-код: 9827-9904

^b кандидат экономических наук, доцент кафедры экономики предприятий и организаций, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского (ННГУ), Нижний Новгород, Российская Федерация
ludushkina@mail.ru
<https://orcid.org/0000-0002-7590-5416>
SPIN-код: 1717-6080

^c кандидат экономических наук, доцент кафедры экономики предприятий и организаций, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского (ННГУ), Нижний Новгород, Российская Федерация
ekornilova89@mail.ru
<https://orcid.org/0000-0001-7852-4945>
SPIN-код: 1023-9412

^d кандидат экономических наук, доцент кафедры экономики предприятий и организаций, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского (ННГУ), Нижний Новгород, Российская Федерация
mvkislinskaya@yandex.ru
<https://orcid.org/0000-0001-5880-6646>
SPIN-код: 1213-3385

* Ответственный автор

История статьи:

Рег. № 118/2021
Получена 11.03.2021
Получена в доработанном виде 24.03.2021
Одобрена 02.04.2021

Аннотация

Предмет. В статье представлен обзор последних результатов зарубежных и отечественных исследований, посвященных обеспечению безопасности сложных экономических систем в процессе их цифровой трансформации. В ходе развертывания технологий Индустрии 4.0 частота, разнообразие и уровень цифровых рисков растут быстрее, чем развиваются средства обеспечения цифровой безопасности сложных систем. Это нейтрализует

* Исследование выполнено в рамках базовой части государственного задания Минобрнауки России, проект № 0729-2020-0056 «Современные методы и модели диагностики, мониторинга, предупреждения и преодоления кризисных явлений в экономике в условиях цифровизации как способ обеспечения экономической безопасности Российской Федерации».

Доступна онлайн
29.04.2021

УДК 658.5

JEL: L20, O32

Ключевые слова:

системы, безопасность,
цифровая
трансформация, риски,
парадигма
безопасности

преимущества цифровой трансформации и может привести к крупномасштабным сбоям.

Цели. Идентифицировать источники новых угроз, уязвимые места сложных систем и возможные потери, оценить результативность предпринятых мер и сформировать современную парадигму обеспечения цифровой безопасности сложных систем.

Методология. Выявление, системный анализ и обсуждение взаимосвязей между последними научными результатами по данной теме, которые позволяют вскрыть методологические проблемы и определить направления их решения для обеспечения цифровой безопасности на качественно новом уровне.

Результаты. Выявлены особенности поведения сложных систем, формирующие системные риски. Идентифицированы тенденции, изменяющие ландшафт цифровых рисков. Рассмотрены классификации уязвимостей и возможных потерь предприятий в процессе их цифровой трансформации. Выявлены пробелы в организационных возможностях по удовлетворению требований цифровой безопасности. Показано, что все более сложная цифровая среда заставляет предприятия перестраивать планы обеспечения непрерывности бизнеса, реагирования на шоки и последующего восстановления. Полученные результаты направлены на повышение цифровой безопасности критически важных видов деятельности сложных систем и более полное использование преимуществ их цифровой трансформации.

Выводы. В ближайшее десятилетие предприятия кардинально изменятся, и им потребуется новая парадигма обеспечения безопасности, органично сочетающая экономический и социальный аспекты, стратегический и оперативный подходы к управлению рисками цифровой трансформации, рассматривающие управление безопасностью как гибкую самообучающуюся экосистему.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2021

Для цитирования: Захаров В.Я., Лудушкина Е.Н., Корнилова Е.В., Кислинская М.В. Безопасность сложных экономических систем: управление рисками их цифровой трансформации // Экономический анализ: теория и практика. – 2021. – Т. 20, № 4. – С. 592 – 623.
<https://doi.org/10.24891/ea.20.4.592>

Введение. Новые возможности и новые риски цифровой трансформации

Все большая часть деятельности многих предприятий зависит от использования цифровых технологий. В последние два десятилетия эта зависимость растет в связи с ускорением цифровой трансформации предприятий на основе цифровых технологий Индустрии 4.0, таких как анализ больших данных, интернет вещей (интернет всего), искусственный интеллект, «умные» дома, предприятия и города, аддитивное производство, дополненная реальность и др.

Все более очевидными для бизнеса становятся преимущества и выгоды технологий четвертой промышленной революции. На цифровую экономику сейчас приходится почти треть ВВП развитых стран по сравнению с менее чем 3% десять лет назад, отмечают исследователи Кембриджского университета [1]. Анализ трендов развития цифровой экономики в России проведен в работах Национального

исследовательского университета «Высшая школа экономики»¹ и МкКинзи². Цифровая трансформация рассматривается руководителями крупных компаний как важная стратегия повышения эффективности и безопасности бизнеса. Как показал опрос, проведенный в 2019 г. компанией Deloitte совместно с Wakefield Research (опрошено 500 руководителей высшего звена, которые несут ответственность за кибербезопасность в компаниях с годовым доходом не менее 500 млн долл.), в качестве актуальных руководители предприятий называют инициативы цифровизации, представленные на рис. 1.

Цифровая трансформация снимает одни риски и создает другие, меняя структуру и интенсивность рисков. Сегодня ущерб от киберпреступности оценивается в 6 трлн долл. в год, это почти 10% мировой экономики³. Общие глобальные расходы на кибербезопасность в настоящее время достигли 145 млрд долл. в год и, по прогнозам, превысят 1 трлн долл. к 2035 г.⁴.

Развертывание Индустрии 4.0 приводит к повсеместному усилению взаимозависимости предприятий. Согласно прогнозу, количество установленных устройств, подключенных к интернету вещей, во всем мире с 2015 по 2025 г. вырастет с 15,4 млрд до 75,4 млрд⁵. Интернет вещей усилил динамику и воздействие цифровых угроз. Устройства интернета вещей (IoT) участвуют в выполнении наиболее значимых для устойчивого развития экономики задач, включая управление генерацией и распределением электроэнергии, очистку воды, химическое производство и переработку, автоматизированные сборочные линии; именно устройства IoT нередко становятся наиболее уязвимыми в системах. Слияние информационных и операционных технологий вызвало появление новых областей (поверхностей) цифровых угроз.

Многие правительства ожидают роста частоты возникновения и серьезности нарушений цифровой безопасности, что может привести к крупномасштабным бедствиям. Согласно опросу руководителей предприятий S&P Global 451, проведенному в октябре 2020 г., пандемия COVID-19 более всего усилила приоритетность таких задач, как информационная безопасность (45% опрошенных),

¹ Доклад «Цифровая экономика: глобальные тренды и практика развития российского бизнеса». URL: https://imi.hse.ru/pr2017_1

² Цифровая Россия: новая реальность. Исследование компании МакКинзи. URL: <https://www.mckinsey.com/~media/mckinsey/locations/europe%20and%20middle%20east/russia/our%20insights/digital%20russia/digital-russia-report.ashx>

³ US Department of Homeland Security, Secretary Kirstjen M. Nielsen Remarks at the RSA Conference, April 17, 2018. URL: <https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference#1>

⁴ The World Economic Forum. Future Series: Cybersecurity, Emerging Technology and Systemic Risk. 2020. URL: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

⁵ Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025. URL: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

непрерывность и устойчивость бизнеса (42%), 71% специалистов по безопасности сообщили об увеличении цифровых угроз с момента начала блокировок⁶.

Ландшафт цифровых угроз постоянно меняется, становится все более разнообразным и технически сложным. Вредоносные программы способны автоматически атаковать уязвимые устройства и распространяться без вмешательства человека. Инструменты взлома систем безопасности постоянно дорабатываются и обновляются, становятся более изощренными и действенными; на их развитие влияют скорость технологических изменений, сложность и защищенность объектов атак, цели и последствия атак. Новый ландшафт угроз вызвал волну крупномасштабных многовекторных мегаатак пятого поколения (с признаками киберпандемии), в то время как системы цифровой безопасности большинства предприятий относятся ко второму и третьему поколениям. Эксперты Всемирного экономического форума полагают, что кибербезопасность стала приоритетом национальной безопасности⁷.

Для максимального использования потенциала новых цифровых технологий необходимо обеспечить безопасность предприятий на качественно новом уровне, создавая надежную защиту в долгосрочной перспективе (безопасность пятого поколения). Если первоначально цифровая безопасность рассматривалась как проблема для ИТ-команды, то в наши дни она стоит на повестке дня высшего руководства компаний и правительств. Некоторые исследователи отмечают, что с увеличением размера и сложности экономических систем (к примеру, городов) расходы на обеспечение их безопасности могут расти более высокими темпами, чем повышение эффективности сложных систем в результате их цифровизации.

Проблему исследования мы видим в том, что возрастание в процессе цифровой трансформации предприятий частоты, разнообразия и интенсивности воздействия цифровых угроз требует принятия новой парадигмы обеспечения безопасности, реализация которой позволит снизить до приемлемого уровня цифровые риски и воспользоваться всеми преимуществами цифровизации в критически важных секторах экономики.

Нами выполнен обзор результатов последних исследований ведущих российских и зарубежных аналитических центров по вопросам обеспечения безопасности предприятий в процессе их цифровой трансформации.

Наша цель – обсудить теоретические рамки новой парадигмы цифровой безопасности предприятий и, опираясь на лучшие практики цифровой трансформации из разных стран, дать рекомендации по усилению этой безопасности.

⁶ 2021 Technology Preview – A Pivotal Year for IT in Preparation for a Postpandemic New Normal.
URL: <https://www.spglobal.com/marketintelligence/en/documents/2021-technology-preview-a-pivotal.pdf>

⁷ Pipikaite A, Barrachin M., Crawford S. These are the Top Cybersecurity Challenges of 2021.
URL: <https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/>

Рассматриваются особенности поведения сложных систем, источники цифровых рисков; виды цифровых уязвимостей и потерь; анализируются контуры современной парадигмы обеспечения безопасности и основные направления действий по безопасному внедрению технологий Индустрии 4.0.

Особенности поведения сложных систем

Общепризнано, что предприятия являются сложными системами, одновременно техническими, экономическими и социальными. Опыт показывает, что провалившихся проектов цифровой трансформации предприятий гораздо больше, чем успешных. Сложность предприятия (количество и взаимозависимость составляющих его элементов) под влиянием ускоряющегося потока новых, в том числе цифровых, технологий, как правило, растет быстрее, чем изменяются сложность управляющей системы, ее представления об объекте управления и инструменты управления. Это порождает разрыв между требованиями к безопасности систем и возможностями их обеспечения; возникают угрозы и системные риски, вызывающие неудачи в реализации проектов цифровой трансформации сложных систем и проблемы в реагировании на шоки и последующем восстановлении.

Сложные системы отличаются большой взаимозависимостью элементов (которую трудно распознать) и нелинейными реакциями; в нелинейной среде, как считают некоторые исследователи, простые причинные связи – скорее аномалия. В сложных системах возможны неуправляемые цепные реакции, которые снижают предсказуемость их поведения и порождают непредвиденные события. На непрозрачное и наивное управление (вмешательство) сложная система может ответить взрывным каскадом неожиданных ветвящихся реакций, каждая из которых опаснее предыдущей, о чем предупреждает Н. Талеб [2].

Сложные системы могут нуждаться во встряске и стрессорах – колебания очищают систему. Такие системы используют встряски как информацию об угрозах и отвечают на нее, воспользуемся формулировкой Н. Талеба, гиперкомпенсацией или многоуровневой избыточностью; система создает новые мощности и копит силы в ожидании худшего исхода, реагируя на сообщения о возможной опасности. Стабильность системы – бомба замедленного действия [2].

В мире Индустрии 4.0 цифровые технологии взаимосвязаны, связи между ними нередко скрыты от нас, в частности, потому, что многие из этих технологий еще не зрелы и хрупки; поведение таких технологий трудно оценить.

Анализ опыта трансформации сложных систем привел Дж. Форрестера к выводу о том, что существуют точки в сложной системе, небольшие изменения в которых могут привести к ее трансформации [3]:

- существуют критические для системы параметры, изменение которых приводит к трансформации поведения системы; обычно системы не приближаются к критическим значениям параметров;
- можно изменить поведение системы, изменяя структуру и размеры ее материальных запасов и потоков;
- для сохранения состояний системы в безопасных пределах при воздействии шоков используются петли обратной связи; силу обратной связи можно изменять относительно силы внешних шоков: при усилении шоков обратная связь усиливается; задержки в обратной связи являются причиной колебаний в поведении системы («недолет» или «перелет»);
- ускорять или замедлять развитие системы возможно с помощью контура положительной обратной связи, меняя коэффициент усиления в ней;
- своевременно изменяя (восстанавливая или дополняя) направление и скорость информационных потоков (кто к какой информации имеет доступ), мы можем предотвращать или смягчать сбои в системе;
- самые глубокие сбои в системах могут быть вызваны неадекватностью правил системы (стимулов, наказаний, ограничений); власть над правилами позволяет активно влиять на трансформацию системы;
- возможность создавать и изменять структуру системы позволяет со временем кардинально изменить систему и ее поведение; способность к самоорганизации – важнейший фактор устойчивого развития системы;
- возможность устанавливать и изменять цели для всей системы – сильнейший рычаг трансформации ее поведения;
- способность изменять парадигму системы, ее ценности, убеждения, видение, нормы позволяет полностью трансформировать систему без больших затрат.

Тенденции, изменяющие ландшафт рисков цифровой безопасности

Для успешного управления рисками цифровой безопасности компании должны уметь идентифицировать, отслеживать и анализировать тенденции, которые формируют будущий ландшафт рисков. Цифровые риски растут и изменяются, они будут выглядеть по-разному для каждого этапа цепочки создания стоимости и каждого предприятия. Анализ тенденций развития рисков позволит компаниям быть на шаг впереди, предотвращать или смягчать возможные последствия кибератак в условиях, когда изменения в рисках цифровой трансформации ускоряются.

Факторы изменения ландшафта рисков:

- новые технологии;

- количество и типы уязвимых систем;
- стратегии, которые используют хакеры для достижения своих целей;
- реакции и технологии обеспечения безопасности предприятий.

Исследования, проведенные Кембриджским университетом и другими ведущими исследовательскими центрами, позволяют выделить следующие ключевые тенденции, изменяющие ландшафт цифровых рисков [1].

Повышение подверженности цифровым атакам и нарушениям. Уже сегодня подключенные цифровые технологии поддерживают критически важные производственные процессы, усиливая их взаимосвязанность, интегрированность, повышая их уязвимость и расширяя фронт (поверхность) для внешних кибератак. Добавление новых портов в сеть компании, поляризация распределения программного обеспечения между локальными технологиями и облачными, стандартизация вокруг ведущих программных продуктов отрасли, интеграция потоков данных в централизованные пакеты ERP и производственные информационные системы повышают эффективность предприятий, расширяют потенциал возможных системных сбоев, делают предприятия более уязвимыми к кибератакам. Даже одной точки взлома может быть достаточно, чтобы поставить под угрозу всю сеть IoT.

Исследования говорят о высокой частоте кибератак: практически все (95%) опрошенные руководители высшего звена признают, что их компании подвергались широкому спектру кибератак; более половины (57%) компаний подверглись нападениям в течение последних двух лет, в том числе 9% – в течение последнего года (рис. 2).

Повсеместная и все более сложная цифровая среда заставляет предприятия переосмыслить планы обеспечения непрерывности бизнеса, реагирования на шоки и последующего восстановления.

Рост электронной торговли и использование Интернета для получения доходов. Подверженность цифровым угрозам наиболее быстро растет в процессе цифровой трансформации розничной торговли и коммерции. Растущая зависимость предприятий от Интернета увеличивает уязвимость бизнес-процессов к сбоям в работе технологий, подключений и взаимосвязанных цепочек поставок систем. У этих компаний есть свои профили рисков, которые требуют подробного анализа.

Повышение вероятности прерывания бизнеса в цифровом пространстве. Атаки на цифровые цепочки поставок. Оцифровка физических активов (создание киберфизической среды) увеличивает поверхность атак цепочек поставок, повышая вероятность того, что одна атака может распространиться на несколько отраслей. Услуги и активы, которые когда-то находились внутри предприятия, переходят к

поставщикам, работающим на цифровой основе. Во всех секторах экономики информационные и операционные технологии распространяются на более интегрированные онлайн/офлайн-среды.

Большинство предприятий работает посредством множественных подключений к сторонним поставщикам, системам технической поддержки и средствам управления потоками данных, которые они не обязательно контролируют, часто даже не видят. Атака на крупные компании через слабые места в безопасности их мелких поставщиков – более простой способ нарушить работу крупной компании, чем взломать ее напрямую [1]. Злоумышленники все чаще используют сторонних партнеров по цепочке поставок для доступа к целевым сетям, особенно когда экосистемы поставщиков находятся вне контроля целевых для них компаний.

Опрос 2018 г. показал, что каждая атака на цепочку поставок вызывает затраты в размере 1,1 млн долл., в США – 1,27 млн. Американские компании решают проблему в цепочке поставок в среднем за 12 часов, нередко на обнаружение и устранение атаки может потребоваться до 63 часов [1].

В 2017 г. на атаки на операционные производственные системы в Великобритании приходилось 47% всех кибератак. Эти атаки часто носят зондирующий характер, злоумышленники составляют карту производственных сетей для обнаружения критически важных активов.

Энергетические системы особенно подвержены риску из-за их социального и экономического значения [4]. Поставка, переработка и распределение энергии происходят на транснациональном уровне, эти процессы с высокой сложностью увеличивают уязвимость цепочки поставок энергии для случайного и преднамеренного вмешательства, что в свою очередь увеличивает уязвимость всех людей и предприятий, полагающихся на эту поставку энергии.

Атаки цепочки поставок программного обеспечения обычно наблюдаются с использованием троянских приложений и вредоносного кода, скрытого в обновлениях программного обеспечения. Роботы, которых в мире установлено более чем 1,5 млн – очень уязвимые системы. Программное обеспечение, работающее на этих устройствах, часто устаревшее, основано на уязвимых операционных системах и библиотеках, а иногда и располагается на устаревших системах. Злоумышленники в случае успешной атаки могут получить доступ к десяткам тысяч промышленных устройств, и потенциальные последствия атаки могут быть велики.

Эти типы атак увеличили потребность предприятий в страховании от прерывания бизнеса.

Растущий потенциал киберфизических потерь. Наибольшую опасность представляют атаки, нацеленные на критически важную (государственную и

частную) национальную инфраструктуру. Критически важной национальной инфраструктурой называют объекты, информацию, людей, сети и процессы, необходимые для функционирования страны и от которых зависит повседневная жизнь.

Атакам способствуют плохая цифровая гигиена, развитие интернета вещей и ограниченные бюджеты на безопасность. Инфекционные вредоносные программы, такие как программы-вымогатели, все чаще нацелены на критически важную национальную инфраструктуру, требуя оплаты за восстановление зашифрованных файлов или возможностей. После запуска самовоспроизводящейся вредоносной программы ее распространение, как правило, становится неконтролируемым, что создает потери как для предполагаемых, так и для непреднамеренных целей.

Кибератаки становятся все более политическими. Государства используют собственные цифровые возможности и возможности частных компаний, интересы которых совпадают с интересами государства, для промышленного шпионажа (К. Александер назвал цифровой промышленный шпионаж величайшей передачей богатства в истории), кражи интеллектуальной собственности и организации разрушительных атак, приводящих к глобальным сбоям и потерям. Наблюдается рост поддерживаемой государством цифровой активности, направленной на достижение политических целей, к примеру, посредством цифрового вмешательства в выборы и манипуляций в социальных сетях.

Национальные государства стремятся к тому, чтобы цифровые вторжения на территории друг друга были значительно ниже порога начала войны. Страны заключают международные соглашения по ограничению агрессивных цифровых вторжений, чтобы предотвратить эскалацию атак выше порога войны. Разрабатываются долгосрочные стратегии ведения цифровой конкуренции между странами, важный элемент которых – формирование способности защищаться, активно выявляя, преследуя и уничтожая цифровые угрозы до возможных атак. Правительства начали запрещать или ограничивать деятельность компаний, происходящих из соперничающих геополитических государств, чтобы уменьшить киберриски вторжений.

Изменение мотивации злоумышленников. Усиливается финансовая мотивация злоумышленников вследствие повышения доходности кибератак. Более высокие доходы позволяют сформировать хакерские команды с превосходными навыками и большими бюджетами, которые способны обеспечить сильную и постоянную угрозу.

Предприятия, ставшие мишенями для сложных и хорошо обеспеченных ресурсами хакерских групп, с большей вероятностью будут подвергаться крупномасштабным кибератакам, которые потенциально могут привести к большим потерям. Это повышает общий уровень рисков цифровой трансформации предприятий.

Киберпреступники все чаще применяют тактику Living Off the Land или «бесфайловых атак» [1]. Для проникновения в систему используются законные и надежные инструменты или приложения, что исключает необходимость запуска вредоносных файлов для атаки. Бесфайловые вредоносные программы увеличивают вероятность успешного заражения и анонимность группы, снижая риск судебных исков против атакующих и повышая угрозы для корпораций.

Повышение стандартов безопасности в компаниях. Всемирные расходы на информационную безопасность превысили 114 млрд долл. в 2018 г., увеличившись более чем на 12% по сравнению с 2017 г. [1]. Быстрее всего растут инвестиции в превентивные меры цифровой безопасности с использованием искусственного интеллекта и машинного обучения: почти половина предприятий включает меры безопасности, основанные на искусственном интеллекте. Искусственный интеллект резко увеличивает общие затраты на цифровую безопасность и, вероятно, начнется гонка «кибероружия» между предприятиями и преступниками.

По данным SCADA, в 2018 г. количество обнаруженных уязвимостей цифровых технологий, используемых в промышленной среде, увеличилось на 30%. Компании, которые оптимизировали свои процедуры реагирования для как можно более быстрого обнаружения опасности, улучшили свои позиции в области цифровой безопасности и сократили расходы, связанные с прерыванием бизнеса. Однако медианное время, которое требуется промышленным корпорациям для обнаружения проникновения в их системы, неуклонно увеличивалось, и в 2018 г. в среднем по миру оно составляло 101 день [1].

Корпорации, пострадавшие от разрушительных кибератак, не хотят пассивно мириться с нападениями и ищут возможности активно ответить: жертва кибератаки, обнаружив атаку, преследует злоумышленников за пределами корпоративных сетей, стремясь наказать их.

Улучшения в правоохранительной сфере и в нормативной среде. Повышается уровень координации работы по киберсдерживанию между правоохранительными органами и партнерами из частного и государственного секторов внутри стран и между странами, что существенно увеличивает издержки для киберпреступников. В отдельных операциях в борьбе с киберпреступниками участвуют десятки стран.

Общий регламент Евросоюза по защите данных (GDPR) предполагает наложение предупреждений и штрафов на компании, не выполняющие требования по защите данных. В США, Канаде, Европе и Индии действуют строгие правила регулирования конфиденциальности данных; Калифорния стала первым штатом США, принявшим закон о кибербезопасности интернета вещей. Совет Безопасности Российской Федерации разработал серию нормативных актов по обеспечению

информационной безопасности⁸. Сравнительный анализ нормативной среды кибербезопасности в разных странах дается в работах [5–9].

Классификация уязвимостей цифровой безопасности

Обеспечение безопасности предприятия предполагает понимание угроз, уязвимостей и возможных потерь, а также уровней операционных и капитальных затрат, необходимых для защиты сотрудников, клиентов и объектов.

Для классификации уязвимостей систем операционных технологий в производственном секторе Кембриджский центр исследования рисков предлагает учитывать [10]:

- методы кибератак;
- активы операционных технологий, на которые нацелены кибератаки (датчики, приводы, хранилища данных, коммуникационные сети, логика принятия решений, системы безопасности, внешние зависимости);
- уязвимые системы: связанные с операционными технологиями (промышленные системы управления ISC, автоматизированные системы безопасности SIS, промышленный интернет вещей, системы управления энергоснабжением EMS и др.); связанные с информационными технологиями (операционные системы, ERP-системы, системы управления взаимоотношениями с клиентами CRM и др.).

Два типа систем – информационные – и производственные технологии – сталкиваются с различными угрозами и уязвимостями. Риски операционных технологий – самые высокие для производственного сектора экономики, поскольку они связаны с возможными киберфизическими последствиями атак: повреждение или вред, нанесенный сотрудникам, зданиям, оборудованию, продукции и, возможно, клиентам.

Цели цифровых атак на системы операционных технологий, критически важные объекты инфраструктуры – ограничить или исключить их доступность, поставить под угрозу их целостность или снизить конфиденциальность данных (они называются триадой ЦРУ) [10].

Доступность означает обеспечение эффективной и надежной работы ключевых систем и активов; если система недоступна, значит, процесс либо не работает полностью, либо работает не на полную мощность; без доступности систем целостность и конфиденциальность не имеют значения.

Целостность означает защиту от ненадлежащего изменения или уничтожения информации и включает обеспечение подлинности информации. До кибератаки специалисты по безопасности должны быть уверены, что резервные копии законны

⁸ Доступно на сайте Совета Безопасности Российской Федерации. URL: <http://www.scrf.gov.ru/>

и не были изменены. Во время атаки нужно знать, какие данные являются достоверными и целостными, и какие источники данных могут или не могут показать вам, что реально произошло. После атаки критически важно проверить целостность резервных копий по мере их восстановления.

Целью конфиденциальности является предотвращение разглашения информации.

Кембриджский центр исследования рисков в 2018 г. предложил следующий перечень ключевых потенциальных уязвимостей систем операционных технологий [10]:

- срок службы промышленных систем управления больше, чем срок службы ИТ-систем: инженерные системы обычно рассчитаны на срок службы в пять раз дольше, чем базовые ИТ-системы. Инструменты кибератак совершенствуются на протяжении всего срока службы промышленных систем. Постоянная проверка целостности цифровых устройств в течение длительного срока службы имеет решающее значение и является сложной задачей для устаревших систем;
- низкая частота установки исправлений (улучшений) цифровых устройств: сложно исправлять операционные системы и программное обеспечение, чтобы обеспечить функциональность всей системы. Исследования показали, что может пройти до 200 дней, прежде чем будет исправлена средняя по размерам и сложности система;
- низкая безопасность паролей и незашифрованные протоколы: пароли по умолчанию не меняются регулярно. Эта ситуация постепенно улучшается, но многие старые системы все еще используются и уязвимы для кибератак;
- растущее использование промышленного интернета вещей при небезопасном удаленном подключении интеллектуальных устройств приводит к неограниченному доступу в Интернет. Сложно убедиться в целостности устройств промышленного интернета вещей после того, как они будут подключены к Интернету;
- доступ сторонних поставщиков: внешние поставщики часто привлекаются для оказания помощи в различных мероприятиях по технической поддержке (улучшение системы, обучение и профилактическое обслуживание). Это создает дополнительный риск, если поставщик (или его организация-клиент) не придерживается строгой культуры цифровой безопасности. Нужно проверять целостность практики цифровой безопасности поставщика и его следует наказывать за несоблюдение договорных требований в отношении кибербезопасности;
- системы управления предприятием: для обеспечения мониторинга производственных процессов в режиме реального времени в корпоративном

офисе существует система отчетов о времени безотказной работы/простоя и определения результатов производства. Эти системы являются потенциальной точкой входа для злоумышленников, которые пытаются перейти из корпоративной среды в систему управления. Целостность сети после добавления новых устройств и систем имеет решающее значение;

- сетевая архитектура: использование брандмауэров, систем обнаружения вторжений и прав пользователей может повысить или понизить безопасность системы операционных технологий в зависимости от того, как они развернуты. Целостность означает проверку, к каким устройствам какие люди имеют доступ;
- затраты на тестирование: безопасность многих успешных продуктов постоянно улучшается в результате тестирования независимыми профессионалами в этой области. Однако такое тестирование нечасто делается в отношении оборудования операционных технологий, так как оно весьма сложное, имеет низкую узнаваемость за пределами узкого круга инженеров, часто неудобно расположено в удаленных зданиях, на нефтяных платформах или в сверхсекретных местах (к которым нужен специальный допуск), в результате тестирование такого оборудования становится дорогостоящим и трудоемким делом. Поэтому цифровая безопасность оборудования может быть недостаточно изучена. Добавим к этому принцип управления «если не сломалось, не чините», и различия между обслуживанием, обновлением и безопасностью ИТ-систем и технологического оборудования станут очевидными;
- возможность физических последствий: к примеру, повреждение дорогостоящего оборудования, которое сложно заменить с точки зрения логистики.

Практика показывает, ожидания того, что потребители технологий самостоятельно в нужное время и в нужном объеме обновят настройки безопасности, применят эффективные меры противодействия, обновят прошивку своих устройств или изменят пароли устройств по умолчанию, часто оказываются нереальными в силу ряда проблем.

Ответы руководителей компаний на вопрос, что является наиболее сложным аспектом управления цифровой безопасностью в вашей организации, распределились, как это представлено на *рис. 3*.

Как видно, руководители предприятий считают, что существуют заметные пробелы в организационных возможностях для удовлетворения сегодняшних требований цифровой безопасности. Способность руководства правильно и согласованно расставлять приоритеты рисков зависит от того, насколько тесно стратегия цифровой трансформации увязывается с корпоративной стратегией, моделью управления компанией, ее бизнес-моделью. На предприятии несколько подразделений участвуют в управлении рисками цифровой безопасности, их

действия должны быть согласованы в рамках общей концепции, что позволит, согласно оценкам экспертов, сократить вдвое работу по достижению одного и того же результата.

Из данных этого опроса следует, что предприятия не полностью оснащены для действенного решения проблем цифровой безопасности, руководители обращают особое внимание на недостаток квалифицированных кадров и недостаточное финансирование; так, подавляющее большинство (90%) опрошенных указали, что на проведение цифровой трансформации выделяется 10% и менее от общего бюджета компании (рис. 4).

По оценкам, в 2021 г. во всем мире будет 3,5 млн незаполненных вакансий специалистов по цифровой безопасности⁹. Руководителям, отвечающим за цифровую безопасность, придется найти способы компенсировать пустые места. Это трудная задача: нужно учитывать много аспектов работы и много уязвимостей; мало специалистов, способных справиться с этими угрозами. Поэтому в сфере обеспечения цифровой безопасности невелика доля штатных (на полной занятости) сотрудников (рис. 5).

Как видим, 56% опрошенных руководителей компаний указали, что штатные сотрудники составляют менее 20% их киберкоманд.

Говоря об уязвимостях, эксперты обращают внимание на набирающее популярность использование гибридного облака (сочетание локального и облачного), которое может увеличить риски данных, если вы не знаете, где ваши данные собираются, хранятся и у кого есть к ним доступ. Необходимо четко понимать, какие конфиденциальные данные предприятие размещает в облаке и какие средства контроля можно использовать, например, для контроля над риском мультиарендности, когда несколько виртуальных машин используют одно и то же физическое пространство.

Основные поставщики общедоступных облаков делают многое, чтобы снизить вероятность того, что один клиент может получить доступ к данным в другой виртуальной машине, но локальная инфраструктура уязвима, если серверы не настроены должным образом. Изменения, внесенные в одну гибридную облачную среду, могут непреднамеренно повлиять на другую. Две трети взломов учетных записей связаны с облачными клиентами, которые реализовали плохие конфигурации, неправильные настройки и простые пароли, не сумев защитить свои данные.

Вероятность того, что ведущий поставщик облачных услуг полностью отключится, мала, но если такое случится, то это окажет катастрофическое влияние на

⁹ Morgan S. Cybersecurity Labor Crunch to Hit 3.5 Million Unfilled Jobs by 2021.

URL: <https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html>

национальную экономику; более вероятны простои (перерывы) в работе определенных облачных сервисов (в соглашениях об обслуживании надежность услуг фиксируется на уровне 99,9%). Надежность каждой из облачных услуг зависит от надежности других услуг, ибо они взаимосвязаны. Влияние потерь определяется их сроками и первопричинами.

Чтобы понять, как угрозы и уязвимости могут повлиять на компанию, необходимо провести классификацию потерь. Такая классификация может быть полезна для оценки потерь от кибератак в сценарном планировании.

Категории потерь при нарушении цифровой безопасности

Кембриджский центр исследований рисков предложил следующую классификацию ключевых потерь после проведения многочисленных интервью со специалистами по цифровой безопасности и основными страховщиками цифровой безопасности [10].

Нарушение конфиденциальности – стоимость реагирования на событие, связанное с нарушением конфиденциальности (открытие и кража данных), включая уведомление, компенсацию, услуги кредитного контроля и другие обязательства третьих сторон перед затронутыми субъектами данных, ИТ-криминалистику, внешние услуги и внутренние расходы на реагирование, судебные издержки. Издержки утечки данных растут из года в год; в 2018 г. средняя стоимость утечки данных во всем мире составила 3,86 млн долл., что на 6,4% больше, чем в 2017 г.¹⁰. Косвенные потери – отток клиентов, прерывание бизнеса, снижение стоимости акций и репутационный ущерб.

Потеря данных и программного обеспечения – стоимость восстановления данных или программного обеспечения, которые были уничтожены или повреждены.

Отказы сетевых сервисов – ответственность перед третьими сторонами, возникающая в результате нарушений безопасности в ИТ-сети организации или проходящих через нее коммуникаций.

Прерывание бизнеса – упущенная выгода или дополнительные расходы, понесенные из-за недоступности ИТ-систем или данных в результате кибератак или неумышленных сбоев ИТ.

Случайное прерывание бизнеса – прерывание бизнеса в результате сбоя ИТ-системы третьей стороны, например поставщика, коммунального предприятия или внешнего поставщика ИТ-услуг.

¹⁰ IBM Security. Cost of a Data Breach Report 2020.

URL: <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ru/pdf>

Затраты на реагирование на происшествия – прямые затраты, понесенные на расследование и устранение нарушения в целях минимизации потерь. Применимо ко всем остальным категориям/событиям.

Затраты, связанные с нормативным регулированием и защитой – охватывают юридические, технические или судебно-медицинские услуги, необходимые для оказания помощи держателю полиса в ответах на правительственные запросы, связанные с кибератакой. Обеспечивают покрытие штрафов, пеней, расходов на защиту, расследований или других регулирующих действий в случаях нарушения закона о конфиденциальности и других затрат, связанных с соблюдением требований регулирующих органов и отраслевых ассоциаций. Страховое возмещение предоставляется там, где это допустимо.

Ответственность: продукт и операции – обязательства перед третьими сторонами, возникающие в отношении ответственности за качество продукции и дефектных операций.

Ответственность: технологические ошибки и упущения – покрытие претензий третьих лиц, связанных с неспособностью предоставить адекватные технические услуги или технические продукты, включая судебные издержки и расходы по обвинениям в результате кибератаки или сбоя ИТ.

Ответственность: ошибки и отсутствие профессиональных услуг – покрытие претензий третьих лиц, связанных с неспособностью предоставить соответствующие профессиональные услуги или продукты (за исключением технических услуг и продуктов), включая судебные издержки и расходы по обвинениям в результате кибератаки или сбоя ИТ.

Ответственность: директора и должностные лица – затраты на компенсацию требований к отдельным должностным лицам предприятия, в том числе за злоупотребление доверием или нарушение обязанностей в результате инцидентов, связанных с цифровым пространством, которые могут возникнуть в результате предполагаемого неправомерного поведения или бездействия компании, ее сотрудников и акционеров.

Обязательства в отношении мультимедиа (клевета, унижение и т.п.) – расходы на расследование, защиту и гражданские убытки, возникшие в результате клеветы, навета, оговора, нарушения авторских прав/товарных знаков, небрежности при публикации любого контента в электронных или печатных средствах массовой информации, а также нарушения прав интеллектуальной собственности третьей стороны.

Финансовые кражи и мошенничество – прямые финансовые потери, понесенные организацией в результате использования компьютеров для совершения мошенничества или кражи денег, ценных бумаг или другого имущества.

Репутационный ущерб – потеря доходов в результате увеличения оттока клиентов или уменьшения объемов транзакций, что может быть напрямую связано с информацией о конкретном нарушении безопасности.

Кибер-вымогательство – стоимость экспертного обслуживания в случае вымогательства в сочетании с суммой выкупа.

Кража интеллектуальной собственности – снижение стоимости актива интеллектуальной собственности, выраженное в виде потери дохода в результате сокращения доли рынка.

Ущерб окружающей среде – покрытие затрат на очистку, восстановление, связанных с вызванными кибернарушениями разливом или выбросом в окружающую среду.

Ущерб физическим активам – убытки, связанные с уничтожением или повреждением физического имущества в результате кибератак.

Смерть и телесные повреждения – ответственность перед третьими лицами за смерть и телесные повреждения в результате кибератак.

Среди руководителей компаний существует консенсус в отношении того, что потеря доходов из-за сбоев в работе и потеря доверия клиентов являются самым большим воздействием кибератак на организации (рис. 6).

Контуры современной парадигмы обеспечения безопасности

Цель государственной политики цифровой безопасности – поддержание непрерывности, устойчивости и безопасности критически важных операций без ограничения преимуществ цифровой трансформации. У любого предприятия и любого государства недостаточно ресурсов для защиты всех данных и всей инфраструктуры. Компании и государства сосредотачиваются на защите наиболее ценных, критически важных для устойчивого развития активов, нарушения в работе которых могут привести к крупномасштабным бедствиям, чтобы сохранялась возможность использовать преимущества технологий Индустрии 4.0, и не налагалось ненужное бремя на остальные виды деятельности¹¹ [11].

Исследования показывают, что с 2004 по 2016 г. 32% крупных компаний испытали серьезное ухудшение общей доходности акционеров (TSR) относительно среднеотраслевого уровня, и только четверть из них смогла успешно восстановиться, превзойдя показатели отрасли в краткосрочной и долгосрочной перспективе. Компании в турбулентной корпоративной среде с большей

¹¹ OECD (2020), Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456. 2021. URL: <https://www.google.com/search?q=OECD+recommendation+on+digital+security+of+critical+activities&sa=X&ved=2ahUKEwiGodPsso7vAhUytYsKHbY6BH0Q3rMBegQIAxAC&biw=1920&bih=979>

вероятностью нуждаются в трансформации, чем компании в стабильной конкурентной среде¹².

В конечном счете речь идет об обеспечении экономического и социального процветания, повышении благосостояния страны и ее граждан. Исходя из этого в 2019 г. рабочая группа ОЭСР по безопасности и конфиденциальности в цифровой экономике предложила перейти от чисто технического подхода к управлению рисками цифровой безопасности к более широкому системному подходу, учитывающему экономический и социальный аспекты управления безопасностью¹³.

Стратегия трансформации предприятий и отраслей основывается на использовании возможностей цифровых технологий Индустрии 4.0, но направляется она видением того, во что трансформируются экономические системы. Исследователи Бостонской консалтинговой группы считают, что на протяжении ближайших 10 лет предприятия кардинально изменятся, чтобы стать успешными в новой цифровой среде; они превратятся в обучающиеся организации нового (третьего) поколения. Компании меняют свою природу, приобретают новые ключевые свойства или функции, и им требуется новая парадигма обеспечения их безопасности. Выделяются следующие новые ключевые функции¹⁴.

Способность предприятий обучаться с разной скоростью. С одной стороны, обновления цифровых технологий требуют высокой скорости обучения в процессе трансформации. Данные с цифровых датчиков поступают в алгоритмы искусственного интеллекта, которые обрабатывают информацию в режиме реального времени и подключены к производственным системам, оптимизируя их работу в постоянно изменяющихся условиях. Организации обретают способность учиться со скоростью алгоритмов.

С другой стороны, все более сильное влияние на развитие компаний оказывают медленные сдвиги во внешней среде (социальные и политические изменения, сдвиги в потребительских предпочтениях и др.).

Системы управления безопасностью должны быть гибкими и интегрированными во времени: обладать способностью видеть риски (потенциальные потери), уязвимости (слабые места) и определять меры реагирования на процессы, развивающиеся с разной скоростью в разных временных периодах (дни, месяцы, годы, десятилетия).

¹² Reeves M., Fæste L., Whitaker K., Hassan F. The Truth About Corporate Transformation. URL: <https://sloanreview.mit.edu/article/the-truth-about-corporate-transformation/>

¹³ OECD (2020), Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456. 2021. URL: <https://www.google.com/search?q=OECD+recommendation+on+digital+security+of+critical+activities&sa=X&ved=2ahUKEwiGodPsso7vAhUytYsKHbY6BH0Q3rMBegQIAxAC&biw=1920&bih=979>

¹⁴ Bailey A., Reeves M., Whitaker K., Hutchinson R. The Company of the Future. URL: <https://www.bcg.com/ru-ru/publications/2019/company-of-the-future>

Это означает органичное сочетание стратегического и оперативного подходов к управлению рисками цифровой безопасности для критически важных видов деятельности¹⁵:

- определение четких целей по укреплению цифровой безопасности и устойчивости критически важных видов деятельности, согласованных на национальном, региональном, отраслевом и корпоративном уровнях;
- использование механизмов управления, которые распределяют полномочия и ответственность между конкретными субъектами, отвечающими за разработку и реализацию политики повышения цифровой безопасности критически важных видов деятельности внутри и между секторами;
- обеспечение общегосударственной координации внутри страны (внутриправительственное сотрудничество, согласованность мер, принимаемых в разных секторах, эффективное распределение ресурсов).

Создание киберфизических (гибридных) интеллектуальных систем, в которых машины могут учиться и адаптироваться, расширяя свое участие в трансформации предприятий и управлении их безопасностью. Гибридные обучающиеся организации сочетают в себе преимущества машин (способность машин быстро определять сложные шаблоны в больших данных) и людей (способность людей декодировать сложные причинно-следственные связи и видеть новые возможности).

Такие технологии активной защиты, как аналитика больших данных, обнаружение аномалий, машинное обучение и искусственный интеллект, позволяют организациям в режиме реального времени получать более широкую картину меняющегося ландшафта угроз и быстро реагировать.

Люди и алгоритмы обладают разной пропускной способностью и сложностью действий, для предупреждения возможных сбоев важен выбор правильных интерфейсов, позволяющих людям понимать и проверять действия машин, и уровня сжатия взаимосвязей между людьми и компьютерами¹⁶.

Расширение экосистем, цифровых платформ – сложных, подвижных сетей организаций с большим количеством партнеров из разных отраслей. Экосистемы позволяют больше экспериментировать и быстрее разрабатывать новые предложения в ответ на возникающие возможности и угрозы. Семь самых крупных глобальных компаний являются цифровыми платформами¹⁷ [12].

¹⁵ OECD (2020), Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456. 2021. URL: <https://www.google.com/search?q=OECD+recommendation+on+digital+security+of+critical+activities&sa=X&ved=2ahUKEwiGodPso7vAhUytYsKHbY6BH0Q3rMBegQIAxAC&biw=1920&bih=979>

¹⁶ Bailey A., Reeves M., Whitaker K., Hutchinson R. The Company of the Future. URL: <https://www.bcg.com/ru-ru/publications/2019/company-of-the-future>

¹⁷ Fuller J., Jacobides M.G., Reeves M. The Myths and Realities of Business Ecosystems. URL: <https://sloanreview.mit.edu/article/the-myths-and-realities-of-business-ecosystems/>

Исследования показывают, что самым сильным риском сотрудничества в экосистемах является кража или потеря данных: более двух третей экспертов (60–70%) из США, Китая, Германии, Японии и Южной Кореи и 85% экспертов из России назвали недостаточную защиту данных основным риском развития сотрудничества [13].

Рассматривая свою деятельность как гибкую, развивающуюся экосистему, предприятия смогут справиться с гораздо большей динамичностью и сложностью процессов, превращаясь в «самонастраивающуюся» организацию, которая постоянно учится и развивается в соответствии со своей средой.

Соответственно, управление безопасностью систем превращается в гибкую самообучающуюся экосистему, способную противостоять изохронным, крупномасштабным многовекторным мегаатакам, разрушающая активность которых распространяется внутри организации и между ними за несколько минут. Для борьбы с киберпреступностью нужна виртуальная деревня. Даже самые лучшие компании, ориентированные на кибербезопасность, могут быть подорваны искушенными и сильными преступниками. Нарушения безопасности могут затронуть весь сектор, и работа с коллегами и конкурентами может иметь решающее значение для системной устойчивости всей отрасли.

Устойчивое развитие во все более динамичной и неопределенной среде, перестройка для этого управления и лидерства. Разного рода шоки (экологические, социальные и экономические) происходят все чаще и наносят все больший ущерб предприятиям; корпоративное долголетие уменьшается, компании падают со своих конкурентных вершин быстрее, чем когда-либо; усиливается конкуренция за устойчивость, именно устойчивость развития становится важнейшей характеристикой безопасности предприятий. Устойчивость понимается как способность компании восстанавливаться до прежнего уровня благополучия и выше после шока благодаря наращиванию ее поглощающего, адаптационного и трансформационного потенциалов, перестраиваясь с помощью новых технологий.

Наращивать общий потенциал управления рисками цифровой безопасности и обеспечения устойчивости (resilience) критически важных видов деятельности возможно посредством¹⁸:

- разработки новых или усиления существующих организационных возможностей реагирования на нарушения – групп реагирования или центров операционной безопасности, отвечающих за мониторинг, предупреждение, оповещение и выполнение мер по восстановлению;

¹⁸OECD (2020), Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456. 2021. URL: <https://www.google.com/search?q=OECD+recommendation+on+digital+security+of+critical+activities&sa=X&ved=2ahUKEwiGodPsso7vAhUytYsKHbY6BH0Q3rMBegQIAxAC&biw=1920&bih=979>

- содействия более быстрому и эффективному сотрудничеству в использовании передовых методов управления рисками цифровой безопасности, международных стандартов цифровой безопасности, обмена информацией об угрозах, уязвимостях и практике управления рисками; определения уровней рисков, которые необходимо снизить, передать, избежать или принять;
- содействия развитию мирового рынка услуг и продуктов в области безопасности;
- поддержки развития квалифицированных кадров, способных управлять корпоративными, отраслевыми и межотраслевыми рисками цифровой безопасности;
- возложения ответственности за управление рисками цифровой безопасности на высший уровень руководства и включение управления рисками цифровой безопасности в общую структуру управления рисками предприятия;
- принятия стратегических целей и планов восстановления для обеспечения непрерывности бизнеса, антикризисного управления и аварийного восстановления; регулярного тестирования и улучшения этих планов, в том числе путем организации корпоративных, отраслевых, межотраслевых и трансграничных учений.

Лидерство концентрируется на приоритизации технологий, обеспечении доверия и этичности поведения. Чем больше разнообразие талантов, идей и источников роста в организации, тем выше ее устойчивость к шокам и ее безопасность в долгосрочной перспективе.

Заключение

Признается, что риски цифровой безопасности возникают в результате потенциальных преднамеренных или непреднамеренных угроз, которые носят трансграничный характер; возникают общие риски цифровой безопасности, которые ни один субъект не может значительно уменьшить для всех; каждый субъект, следовательно, зависит от всех остальных и несет ответственность перед ними за управление рисками цифровой безопасности. Сбои в выполнении критически важных операций, вызванные нарушениями цифровой безопасности в одном месте, могут каскадом распространяться на других операторов, другие секторы и страны.

Для повышения цифровой безопасности потребуется адаптация общих политических рамок, построение доверительных отношений и улучшение сотрудничества на всех уровнях: корпоративном, отраслевом, национальном и международном. Несоответствия в государственной политике безопасности в разных странах усложняют управление цифровой безопасностью важнейших видов деятельности.

И государственный, и частный секторы участвуют в обеспечении экономической безопасности. И частному сектору понадобится то, что способна сделать только государственная сфера (правительство): разработка общей политики безопасности, моделей стимулирования безопасного поведения, формирующие рынки, широкомасштабное обучение.

Киберпреступники не останавливаются на границах отраслей и стран, не подчиняются различным юрисдикциям. Между тем предприятиям необходимо ориентироваться в постоянно усложняющейся системе нормативных положений и правил, действующих в разных странах, которые могут содержать разные, а иногда и противоречивые приоритеты, что может ослабить механизмы защиты и повысить затраты для компаний на безопасность.

Нормы конфиденциальности и защиты данных, безусловно, необходимы: руководители предприятий опасаются, что невысокая безопасность данных приведет к потере ключевых компетенций, которые станут общим достоянием. В России, как и в других странах, обеспокоены безопасностью данных больше малые и средние предприятия [14].

Директивным национальным и международным органам необходимо взвешивать свои решения с учетом их позитивных и негативных последствий: их политики и стратегии должны повышать защиту предприятий при снижении сложности регулирования.

Киберпреступность приносит большие выгоды и мало рисков: до недавнего времени вероятность обнаружения и судебного преследования киберпреступников оценивалась на уровне 0,05% в США. Во многих других странах этот процент еще ниже¹⁹. Очень сложно доказать, что конкретный субъект совершил определенные действия. Это выгодная бизнес-модель и ее нужно сломать совместными усилиями разных стран в процессе взаимодействия между корпорациями, политиками и регулирующими органами. В ближайшем будущем крайне важно добиться, чтобы развитие нового поколения средств кибербезопасности не отставало от быстро растущего ландшафта рисков.

¹⁹ Pipikaite A., Barrachin M., Crawford S. These are the Top Cybersecurity Challenges of 2021.
URL: <https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/>

Рисунок 1

Самые актуальные инициативы цифровой трансформации на ближайший год

Figure 1

Top-ranked digital transformation initiatives for the next 12 months



Источник: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Source: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

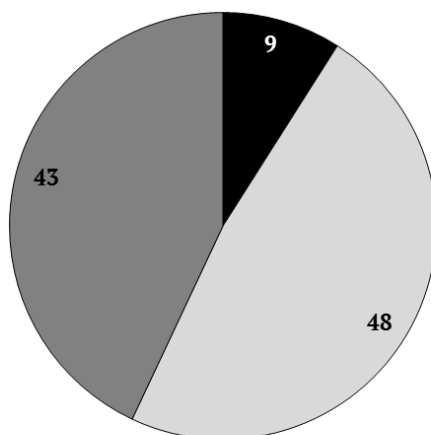
URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Рисунок 2

Распределение последних кибератак во времени (от всех компаний, подвергшихся кибератакам), %

Figure 2

Timing of the most recent cyber attacks (of the total amount of companies that have been attacked), percentage



■ В течение последнего года □ От одного года до двух лет назад ■ Более двух лет назад

Источник: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Source: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Рисунок 3

Наиболее сложные аспекты управления цифровой безопасностью в организации

Figure 3

The most challenging aspects of cyber security management in the organization



Источник: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Source: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

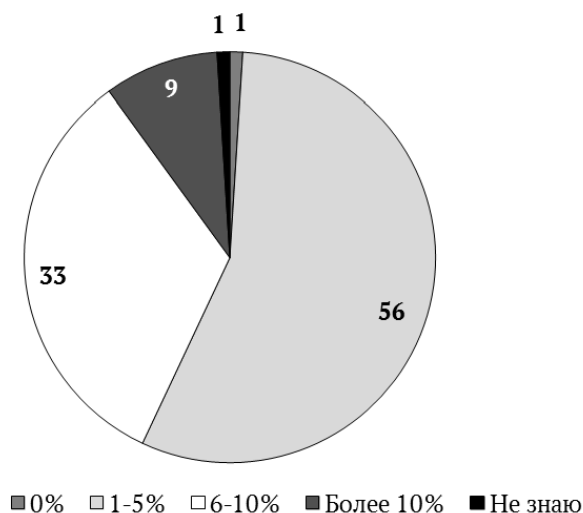
URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Рисунок 4

Доля кибербюджета, выделенного на цифровую трансформацию от общего бюджета

Figure 4

Percentage of cyber budget allocated to digital transformation



Источник: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Source: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

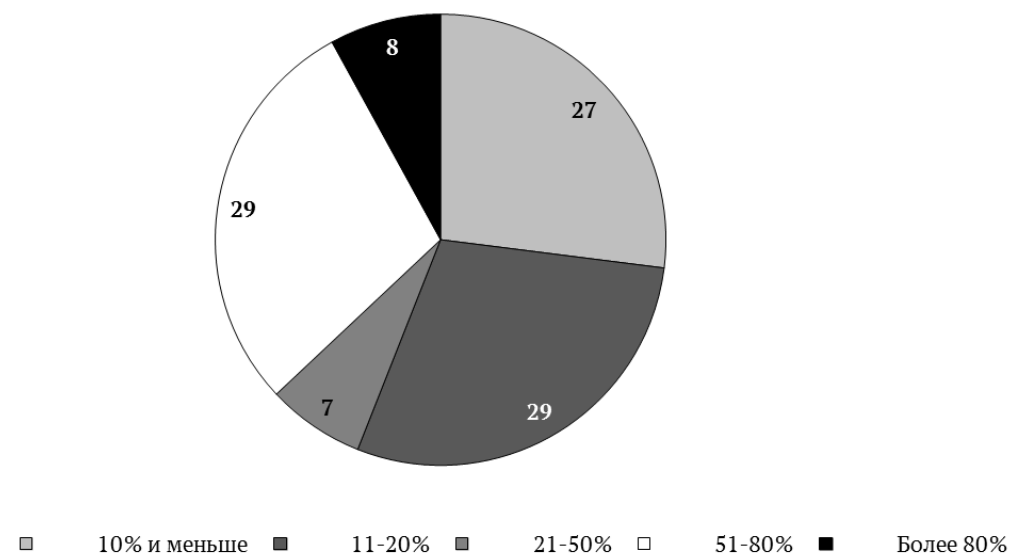
URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Рисунок 5

Доля штатных сотрудников среди персонала, поддерживающего цифровую безопасность

Figure 5

Percentage of full-time cybersecurity employees

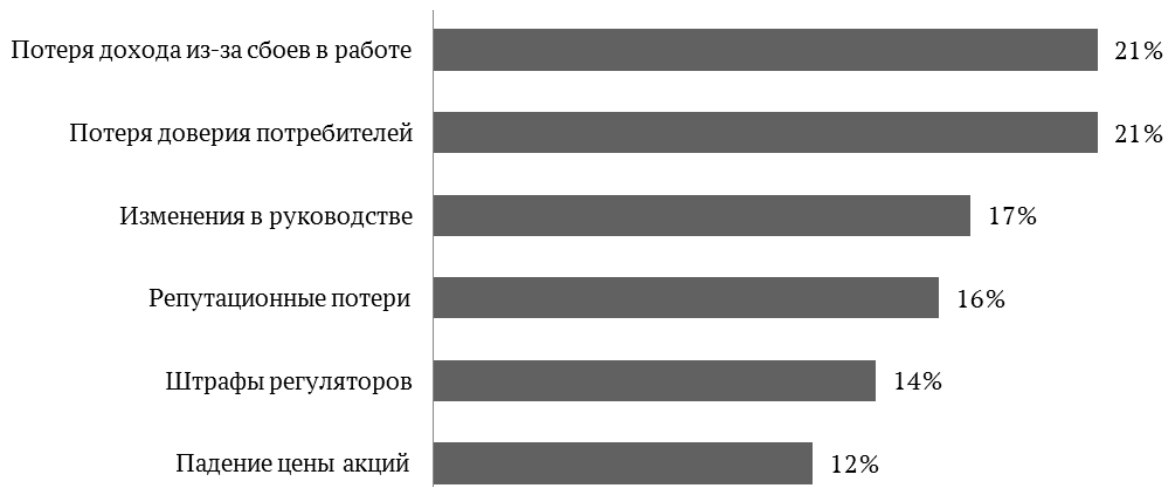


Источник: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Source: The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.

URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>

Рисунок 6**Виды потерь из-за цифровых нарушений, оказывающих наибольшее влияние на организации****Figure 6****The biggest impact of cyber incidents or breaches on organizations***Источник:* The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>*Source:* The Future of Cyber Survey 2019. Cyber Everywhere. Succeed Anywhere.URL: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf>**Список литературы**

1. Coburn A.W., Daffron J., Quantrill K. et al. Cyber Risk Outlook. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc., 2019, 54 p. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf>
2. Талеб Н.Н. Антихрупкость. Как извлечь выгоду из хаоса. М.: КоЛибри, Азбука-Аттикус, 2015. 768 с.
3. Meadows D. Leverage Points: Places to Intervene in a System. *Solutions*, 2010, vol. 1, iss. 1, pp. 41–49. URL: <https://thesolutionsjournal.com/2016/02/22/leverage-points-places-to-intervene-in-a-system/>
4. Малкина М.Ю., Абросимова О.Ю. Анализ особенностей функционирования естественных монополий в современной России // *Экономический анализ: теория и практика*. 2012. № 12. С. 56–64.
URL: <https://cyberleninka.ru/article/n/analiz-osobennostey-funktsionirovaniya-estestvennyh-monopoliy-v-sovremennoy-rossii>
5. Валько Д.В. Киберпреступность в России и мире: сравнительный анализ // *Управление в современных системах*. 2016. № 3.

- URL: <https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka>
6. *Елин В.М.* Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография. М.: Московский институт государственного управления и права, 2016. 121 с.
 7. *Лобач Д.В., Смирнова Е.А.* Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 4. С. 23–32.
URL: <https://cyberleninka.ru/article/n/sostoyanie-kiberbezopasnosti-v-rossii-na-sovremennom-etape-tsifrovoy-transformatsii-obschestva-i-stanovlenie-natsionalnoy-sistemy>
 8. *Курилкин А.В.* Ключевые элементы российской системы противодействия информационным и кибератакам // Русская политология. 2019. № 3. С. 69–73.
URL: <https://cyberleninka.ru/article/n/klyuchevye-elementy-rossiyskoy-sistemy-protivodeystviya-informatsionnym-i-kiberatakam>
 9. *Швырев Б.А.* О безопасности в киберпространстве // Международный журнал гуманитарных и естественных наук. 2021. № 1-1. С. 93–97.
URL: <https://cyberleninka.ru/article/n/o-bezopasnosti-v-kiberprostranstve>
 10. *Copic J., Leverett E.* Managing Cyber Risk in the Fourth Industrial Revolution: Characterising Cyber Threats, Vulnerabilities and Potential Losses. Cambridge Centre for Risk Studies, University of Cambridge, 2019, 24 p.
URL: https://concinuity-risks.com/assets/Briefing_Cyber_Security.pdf
 11. *Малкина М.Ю.* Вклад регионов и отраслей в финансовую нестабильность российской экономики // Terra Economicus. 2018. Т. 16. № 3. С. 118–130.
URL: <https://cyberleninka.ru/article/n/vklad-regionov-i-otrasley-v-finansovuyu-nestabilnost-rossiyskoy-ekonomiki>
 12. *Клейнер Г.Б.* Экономика экосистем: шаг в будущее // Экономическое возрождение России. 2019. № 1. С. 40–45.
URL: <https://cyberleninka.ru/article/n/ekonomika-ekosistem-shag-v-budushee>
 13. *Frolov V.G., Trofimov O.V., Zakharov V.Ya., Pavlova A.A.* Opportunities and Risks from Cooperation among Companies within the Production Sphere and the Sphere of Services in Russia in the Context of Industry 4.0. Amazonia Investiga, 2019, vol. 8, no. 20, pp. 596–608. URL: <https://amazoniainvestiga.info/index.php/amazonia/article/view/190>

14. Трофимов О.В., Захаров В.Я., Фролов В.Г., Павлова А.А. Развитие сложных экономических систем в условиях цифровой трансформации промышленности: теория, методология, практика: монография. М.: Первое экономическое издательство, 2020. 260 с.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

SECURITY OF COMPLEX ECONOMIC SYSTEMS: RISK MANAGEMENT OF THEIR DIGITAL TRANSFORMATION

Vladimir Ya. ZAKHAROV ^a,

Elena N. LUDUSHKINA ^{b,*},

Elena V. KORNILOVA ^c,

Marina V. KISLINSKAYA ^d

^a National Research Lobachevsky State University of Nizhny Novgorod (UNN),
Nizhny Novgorod, Russian Federation
zaxarov48@yandex.ru
<https://orcid.org/0000-0001-6402-4827>

^b National Research Lobachevsky State University of Nizhny Novgorod (UNN),
Nizhny Novgorod, Russian Federation
ludushkina@mail.ru
<https://orcid.org/0000-0002-7590-5416>

^c National Research Lobachevsky State University of Nizhny Novgorod (UNN),
Nizhny Novgorod, Russian Federation
ekornilova89@mail.ru
<https://orcid.org/0000-0001-7852-4945>

^d National Research Lobachevsky State University of Nizhny Novgorod (UNN),
Nizhny Novgorod, Russian Federation
mvkislinskaya@yandex.ru
<https://orcid.org/0000-0001-5880-6646>

* Corresponding author

Article history:

Article No. 118/2021
Received 11 March 2021
Received in revised form
24 March 2021
Accepted 2 April 2021
Available online
29 April 2021

JEL classification: L20,
O32

Keywords: systems,
security, digital
transformation, risk,
security paradigm

Abstract

Subject. The article presents an overview of recent results of foreign and domestic studies on the security of complex economic systems in the process of their digital transformation. During the deployment of Industry 4.0 technologies, the frequency, diversity and level of digital risks are growing faster than digital security tools for complex systems are evolving. This will offset the benefits of digital transformation, and can lead to large-scale failures.

Objectives. The aim is to identify sources of new threats, vulnerability areas of complex systems and possible losses, assess the result of measures taken, and form a modern paradigm for ensuring the digital security of complex systems.

Methods. The study employs identification, systems analysis and discussion of relationship between recent scientific results on this topic that enable to reveal methodological problems and determine the directions of their solution to ensure digital security at a qualitatively new level.

Results. We unveiled the behavior patterns of complex systems, which form systemic risks, identify trends that are changing the digital risk landscape, consider classifications of weaknesses and possible losses of enterprises in the process of their digital transformation, show the gaps in organizational capabilities to meet digital security requirements. The increasingly complex digital environment forces enterprises to redesign their plans for business continuity.

Conclusions. In the next decade, enterprises will need a new paradigm of security, organically combining economic and social aspects, a strategic and operational approach to the risk management of digital transformation, considering the security management as a flexible learning ecosystem.

© Publishing house FINANCE and CREDIT, 2021

Please cite this article as: Zakharov V.Ya., Ludushkina E.N., Kornilova E.V., Kislinskaya M.V. Security of Complex Economic Systems: Risk Management of Their Digital Transformation. *Economic Analysis: Theory and Practice*, 2021, vol. 20, iss. 4, pp. 592–623.
<https://doi.org/10.24891/ea.20.4.592>

Acknowledgments

The study was supported within the framework of the basic part of State job of the Ministry of Education and Science of the Russian Federation, project № 0729-2020-0056, *Modern Methods and Models for Diagnosing, Monitoring, Preventing and Overcoming the Crisis Phenomena in the Economy in the Context of Digitalization as a Way to Ensure the Economic Security of the Russian Federation*.

References

1. Coburn A.W., Daffron J., Quantrill K. et al. Cyber Risk Outlook. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc., 2019, 54 p. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf>
2. Taleb N.N. *Antikhrupkost'. Kak izvlech' vygodu iz khaosa* [Antifragile. Things That Gain from Disorder]. Moscow, KoLibri, Azbuka-Attikus Publ., 2015, 768 p.
3. Meadows D. Leverage Points: Places to Intervene in a System. *Solutions*, 2010, vol. 1, iss. 1, pp. 41–49. URL: <https://thesolutionsjournal.com/2016/02/22/leverage-points-places-to-intervene-in-a-system/>
4. Malkina M.Yu., Abrosimova O.Yu. [Analysis of the special features of the functioning of natural monopolies in modern Russia]. *Ekonomicheskii analiz: teoriya i praktika* = *Economic Analysis: Theory and Practice*, 2012, no. 12, pp. 56–64.
URL: <https://cyberleninka.ru/article/n/analiz-osobennostey-funktsionirovaniya-estestvennyh-monopoliy-v-sovremennoy-rossii> (In Russ.)
5. Val'ko D.V. [Cybercrimes in Russia and the World: Comparative Evaluation]. *Upravlenie v sovremennykh sistemakh*, 2016, no. 3. (In Russ.)
URL: <https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka>
6. Elin V.M. *Sravnitel'nyi analiz pravovogo obespecheniya informatsionnoi bezopasnosti v Rossii i za rubezhom: monografiya* [A comparative analysis of legal support to

- information security in Russia and abroad: a monograph]. Moscow, Moscow Institute of Public Administration and Law Publ., 2016, 121 p.
7. Lobach D.V., Smirnova E.A. [The status of cyber security in Russia at the modern stage of the digital transformation of the company and the formation of the national system of countering cyber threats]. *Territoriya novykh vozmozhnostei. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa = The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2019, vol. 11, no. 4, pp. 23–32.
URL: <https://cyberleninka.ru/article/n/sostoyanie-kiberbezopasnosti-v-rossii-na-sovremennom-etape-tsifrovoy-transformatsii-obschestva-i-stanovlenie-natsionalnoy-sistemy> (In Russ.)
8. Kurilkin A.V. [Key elements of the Russian system of countering information and cyber attacks]. *Russkaya politologiya = Russian Political Science*, 2019, no. 3, pp. 69–73. URL: <https://cyberleninka.ru/article/n/klyuchevye-elementy-rossiyskoy-sistemy-protivodeystviya-informatsionnym-i-kiberatakam> (In Russ.)
9. Shvyrev B.A. [About security in cyberspace]. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*, 2021, no. 1-1, pp. 93–97. URL: <https://cyberleninka.ru/article/n/o-bezopasnosti-v-kiberprostranstve> (In Russ.)
10. Copic J., Leverett E. Managing Cyber Risk in the Fourth Industrial Revolution: Characterising Cyber Threats, Vulnerabilities and Potential Losses. Cambridge Centre for Risk Studies, University of Cambridge, 2019, 24 p.
URL: https://concinntity-risks.com/assets/Briefing_Cyber_Security.pdf
11. Malkina M.Yu. [Contribution of regions and their sectors to the financial instability of the Russian economy]. *TERRA ECONOMICUS*, 2018, vol. 16, no. 3, pp. 118–130.
URL: <https://cyberleninka.ru/article/n/vklad-regionov-i-otrasley-v-finansovuyu-nestabilnost-rossiyskoy-ekonomiki> (In Russ.)
12. Kleiner G.B. [Ecosystem Economy: Step into the Future]. *Ekonomicheskoe vozrozhdenie Rossii = Economic Revival of Russia*, 2019, no. 1, pp. 40–45.
URL: <https://cyberleninka.ru/article/n/ekonomika-ekosistem-shag-v-budushee> (In Russ.)
13. Frolov V.G., Trofimov O.V., Zakharov V.Ya., Pavlova A.A. Opportunities and Risks from Cooperation among Companies within the Production Sphere and the Sphere of Services in Russia in the Context of Industry 4.0. *Amazonia Investiga*, 2019, vol. 8, no. 20, pp. 596–608. URL: <https://amazoniainvestiga.info/index.php/amazonia/article/view/190>

14. Trofimov O.V., Zakharov V.Ya., Frolov V.G., Pavlova A.A. *Razvitie slozhnykh ekonomicheskikh sistem v usloviyakh tsifrovoi transformatsii promyshlennosti: teoriya, metodologiya, praktika: monografiya* [Development of complex economic systems in the context of digital transformation of the industry: Theory, methodology, practice: a monograph]. Moscow, Pervoe ekonomicheskoe izdatel'stvo Publ., 2020, 260 p.

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.